APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/719,347	12/08/2000	Christophe Declerck	11345-018001	7622

22511 7590 07/20/2004

OSHA & MAY L.L.P.
1221 MCKINNEY STREET
HOUSTON, TX 77010

EXAMINER
LAMBRECHT, CHRISTOPHER M

ART UNIT	PAPER NUMBER
2611	4

DATE MAILED: 07/20/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO 90C (Rev 10/03)

	Application No.	Applicant(s)
Office Action Summary	09/719,347	DECLERCK, CHRISTOPHE
	Examiner	Art Unit	
	Christopher M. Lambrecht	2611	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____ .

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-40* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-40* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on <u>*08 December 2000*</u> is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☒ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____ .

      3.☒ Copies of the certified copies of the priority documents have been received in this National Stage
application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date <u>3</u>.

4)☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____ .

DETAILED ACTION

Claim Objections

1.   Claim 21 is objected to because of the following informalities: On line 1 of claim 21, the word

"any" should be deleted. Appropriate correction is required.

Claim Rejections - 35 USC § 102

2.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis

for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3.   Claim 1-5, 8-14, 17, 20, 22-29, 32-37, and 40 are rejected under 35 U.S.C. 102(b) as being

anticipated by Blatter (Blatter et al., WO 97/46008, supplied by applicant).

        With regard to claims 1 and 25, Blatter discloses a decoder (transport system 25, fig. 1) for and

corresponding method of processing a transport packet stream comprising packetised data encapsulated

within the packet payloads (p. 6, ll. 26-29), said decoder comprising: means (45, fig. 1) for receiving an

identifier (pre-loaded PID) of a particular security module system (p. 7, ll. 18-30) from a portable security

module (smart card system 130) (p. 8, ll. 2-4); means (controller 115, fig. 1) for configuring the decoder

in response to the received identifier (p. 6, l. 33 – p. 7, l. 2, 18-30, & p. 8, ll. 2-4); means (PID detection

filters) for receiving filter data for filtering packetised data associated with said particular security module

system from the potable security module (p. 7, ll. 18-30); and means (45, fig. 1) for filtering said

packetised data in response to said received filter data (p. 7, ll. 21-24).

As for claims 2 and 26, Blatter discloses a decoder and corresponding method according to claims 1 and 25 (see above), wherein the filtering means is configurable to extract from the packetised data data associated with said particular security module system for subsequent filtering in response to said received filter data (p. 7, ll. 25-30).

As for claims 3 and 27, Blatter discloses a decoder and corresponding method according to claims 1 and 25 (see above), wherein said identifier (pre-loaded PID) comprises an identifier of a particular conditional access system (pre-loaded PIDs have associated encryption keys, p. 7, ll. 27-30; an encryption key corresponds to a particular conditional access system).

As for claims 4 and 28, Blatter discloses a decoder and corresponding method according to claims 4 and 27 (see above), wherein the filtering means (45) is adapted to extract from the packetised data transport packets containing a program map table and a conditional access table (p. 6, ll. 26-27, p. 10, ll. 10-15 & 32-37).

As for claims 5 and 29, Blatter discloses a decoder and corresponding method according to claims 1 and 25 (see above), wherein the configuring means (controller 115) is adapted to receive the program map table conditional access table (i.e., PSI data, p. 10, ll. 32-37) from the filtering means (45, via unit 60, p. 10, ll. 10-15) and configure the filtering means in response to the received identifier and data contained in the program map table and the conditional access table (p. 11, ll. 13-18).

As for claims 8 and 32, Blatter discloses a decoder and corresponding method according to claims 1 and 25 (see above), wherein the filtering means (45) is configurable (by controller 115) in response to

filter data comprising a table identifier (PIDs 0x0000 and 0x0001 for PAT and CAT tables respectively,

p. 11, ll. 13-20).

As for claims 9, 33, and 34, Blatter discloses a decoder and corresponding method according to

claim 1 and 25 (see above), wherein the filtering means (45) comprises first filtering means for extracting

from the packetised data data associated with said particular security module system (p. 10, ll. 10-15,

where PSI information comprises a conditional access table CAT containing data associated with said

particular security module system, p. 10, ll. 32-36, and p. 11, ll. 10-12) and second filtering means for

filtering the extracted data in response to said filter data (where a PID, i.e., a particular sequence or

pattern of digital data, is a "data pattern") (p. 7, ll. 18-30, i.e., once the pre-load registers of 45 have been

configured by controller 115 with appropriate PIDs (data patterns), PID detection filters of 45 can then

filter (or recognize) extracted data associated with said PIDs (i.e., having matching PID)).

With regard to claims 10 and 35, Blatter discloses a decoder (transport system 25, fig. 1) and

corresponding method for processing a transport packet stream comprising packetised data encapsulated

within the packet payloads (p. 6, ll. 26-29), said decoder comprising: first filtering means for extracting

from the packetised data data associated with a particular security module system (p. 10, ll. 10-15, where

PSI information comprises a conditional access table CAT containing data associated with said particular

security module system, p. 10, ll. 32-36, and p. 11, ll. 10-12); and second filtering means for filtering the

extracted data in response to filter data received from a portable security module (p. 7, ll. 18-30, i.e., once

the pre-load registers of 45 have been configured by controller 115 with appropriate PIDs, PID detection

filters of 45 can then filter (or recognize) extracted data associated with said PIDs (i.e., having matching

PID)).

As for claims 11 and 36, Blatter discloses a decoder and corresponding method according to claims 10 and 35 (see above), wherein the first filtering means is configurable (by controller 115) in response to an identifier of said particular security module system received from said security module (smart card system 130) (p. 7, ll. 18-30, and p. 8, ll. 2-4).

As for claim 12, Blatter discloses a decoder according to claim 9 (see above), wherein said second filtering means comprises a plurality of filters (PID detection filters of 45, p. 7, ll. 18-21), at least one of said filters being configurable (by controller 115) in response to said filter data (p. 7, ll. 18-30, i.e., once the pre-load registers of 45 have been configured by controller 115 with appropriate PIDs, PID detection filters of 45 can then filter (or recognize) extracted data associated with said PIDs (i.e., having matching PID)).

As for claim 13, Blatter discloses a decoder according to claim 9 (see above), wherein said second filtering means is configurable (by controller 115) in response to a data pattern (i.e., PID, where a PID, i.e., a particular sequence or pattern of digital data, is a "data pattern") included in said filter data (p. 7, ll. 18-30, where the filter data comprises pre-loaded PIDs extracted from PSI information by controller 115, p. 10, ll. 10-15).

As for claim 14, Blatter discloses a decoder according to claim 13 (see above), wherein said filtering means is configurable to filter from the extracted data data having a pattern matching said data pattern included in the filter data (p. 7, ll. 18-30, where PID detection filters filter data having PIDs matching those that are pre-loaded by controller 115 in control registers of 45).

As for claims 17 and 37, Blatter discloses a decoder and corresponding method according to claims 1 and 25 (see above), comprising means for forwarding to the security module conditional access data included in the packetised data (p. 8, ll. 2-4).

As for claims 20 and 40, Blatter discloses a decoder and corresponding method (see above) according to claims 17 and 37 (see above), wherein the decoder is adapted to receive a control word (encryption key) generated by the security module (smart card system 130) in response to the conditional access data forwarded thereto (encryption code) (p. 8, ll. 2-9), the control word being used by the decoder to descramble a scrambled transmission (p. 8, ll. 10-18).

As for claim 22, Blatter discloses a portable security module (smart card system 130) for use with a decoder as claimed in claim 1 (see above), said security module comprising memory means for storing an identifier of a particular system of the security module (p. 8, ll. 2-7) and means for communicating the identifier to the decoder to configure the decoder (p. 7, ll. 18-30, where the encryption keys generated by smart card system 130 are used to configure control registers of filtering means 45).

As for claim 23, Blatter discloses a portable security module according to claim 22, comprising means for storing filter data (entitlement information used to derive encryption keys, p. 8, ll. 2-7) and means for communicating the filter data to filtering means in the decoder (p. 7, ll. 18-30, where the encryption keys generated by smart card system 130 are used to configure control registers of filtering means 45).

As for claim 24, Blatter discloses a portable security module according to claim 22 (see above), comprising a smart card (smart card system 130).

Claim Rejections - 35 USC § 103

4.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness

rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5.   Claims 6, 7, 30, and 31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Blatter in

view of Narasimhan (Narasimhan et al., US006237145B1.

With regard to claims 6, 7, 30, and 31, Blatter discloses a decoder and corresponding method

according to claims 1 and 25 (see above). However, Blatter fails to disclose said identifier comprises an

identifier of a particular debiting and crediting system used by the security module.

In an analogous art, Narasimhan discloses an identifier comprising an identifier comprising an

identifier of a particular debiting and crediting system (col. 7, ll. 40-48 & 52-56) used by the security

module (smart card) (col. 7, ll. 10-20), for the purpose of providing a system for electronically debiting

and crediting the user's account (col. 8, ll. 40-56).

Consequently, it would have been obvious to one of ordinary skill in the art at the time the

invention was made to modify the system of Blatter to include said identifier comprises an identifier of a

particular debiting system used by the security module, as taught by Narasimhan, for the purpose of

providing a system for electronically debiting and crediting the user's account in a decoder for a

conditional access system.

6.   Claim 16 is rejected under 35 U.S.C. 103(a) as being unpatentable over Blatter in view of

Anderson (Anderson et al., US006091772A).

With regard to claim 16, Blatter discloses a decoder according to claim 13. However, Blatter fails to disclose said second filtering means is configurable to ignore at least a part of said data pattern in response to a data masking pattern included in said filter data.

In an analogous art, Anderson discloses a filtering means configured to ignore at least a part (4 bytes) of said data pattern in response to a data masking (bit masking) pattern included in said filter data (col. 12, ll. 52-57). By ignoring bits not relevant to the operation being performed, data masking minimizes trivial computations.

Consequently, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the system of Blatter to include said second filtering means is configurable to ignore at least a part of said data pattern in response to a data masking pattern included in said filters, as taught by Anderson, for the purpose of minimizing trivial computations in a decoder for a conditional access system.

7.   Claims 15, 18, 19, 21, 38 and 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Blatter in view of EBU Project Group ("Functional Model of a Conditional Access System", EBU Project Group B/CA, EBU Technical Review Winter 1995, supplied by applicant).

With regard to claim 15, Blatter discloses a decoder according to claim 13 (see above), wherein said filtering means is configurable to filter from the extracted data data having a pattern matching said data pattern included in the filter data (p. 7, ll. 18-30, where PID detection filters filter data having PIDs matching those that are pre-loaded by controller 115 in control registers of 45). However, Blatter fails to explicitly disclose the filtering means is configurable to not filter the data matching said data pattern.

In an analogous art, EBU Project Group discloses configuring a decoder to not descramble any service regardless of authorizations stored in the smart card or other security device (pg. 75, col. 1, ¶1, i.e., disabling any filtering functions involved in the descrambling of services using authorizations associated with the security device & pg. 74, col. 2, section 6). Disabling descrambling functionality at customers' premises increases cable operators control over the network and consequently improves security.

Consequently, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the system of Blatter to include the filtering means is configurable to not filter data matching said data pattern, as taught by EBU Project Group, for the purpose of improving security in a conditional access system.

As for claim 21, Blatter discloses a decoder according to claim 1. However, Blatter fails to disclose the decoder is adapted to encrypt and/or decrypt communications to and from the portable security module.

In an analogous art, EBU Project Group discloses a decoder adapted to encrypt and/or decrypt communications to and from the portable security module (pg. 69, see conditional access sub-system, fig. 6). Encrypting communications to and from the smart card protects private security keys stored within the portable security module.

Consequently, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the system of Blatter to include the decoder is adapted to encrypt and/or decrypt communications to and from the portable security module, as taught by EBU Project Group, for the purpose of protecting private security keys stored within the portable security module in a conditional access enabled decoder.

With regard to claims 18 and 38, Blatter discloses a decoder and corresponding method according to claims 17 and 37 (see above), wherein the conditional access data (encryption codes) forwarded to the security module (smart card system 130) comprises entitlement data (where the encryption codes are processed by smart card system 130 containing entitlement information to generate encryption keys, p. 8, ll. 2-9, the encryption codes extracted from the data stream and forwarded to the smart card system 130). Blatter fails to specifically disclose the entitlement data forwarded to the security module comprises entitlement control messages (ECMs) and/or entitlement management messages (EMMs).

In an analogous art, EBU Project Group discloses data forwarded to the conditional access module comprises entitlement control messages (p. 68, section 3.3), for the purpose of permitting descrambling of scrambled content (p. 68, section 3.3, paragraph 1).

Consequently, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the system of Blatter to include the data forwarded to the conditional access module comprises entitlement control messages, as taught by EBU Project Group, for the purpose of permitting descrambling of scrambled content in a decoder for a conditional access system.

With regard to claims 19 and 39, Blatter discloses a decoder and corresponding method according to claims 1 and 25 (see above), wherein the filter data provided (encryption keys) by the security module (smart card system 130) comprises data used by the filtering means (45, p. 7, ll. 18-21) to extract entitlement data addressed to the security module (where the encryption codes are processed by smart card system 130 containing entitlement information to generate encryption keys, p. 8, ll. 2-9, the encryption codes extracted from the data stream and forwarded to the smart card system 130). Blatter fails to disclose the entitlement data comprises group and/or individual entitlement messages.

In an analogous art, EBU Project Group discloses entitlement data comprising group and/or individual entitlement messages (pg. 69, section 3.4 and pg. 65, col. 1, paragraph 10), for the

purpose providing a viewer with authorization to descramble a particular service (pg. 65, col. 1, paragraph 10).

Consequently, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the system of Blatter to include entitlement data comprising group and/or individual entitlement messages, as taught by EBU Project Group, for the purpose providing a viewer with authorization to descramble a particular service in a decoder for a conditional access system.

Conclusion

8.   The following are suggested formats for either a Certificate of Mailing or Certificate of Transmission under 37 CFR 1.8(a). The certification may be included with all correspondence concerning this application or proceeding to establish a date of mailing or transmission under 37 CFR 1.8(a). Proper use of this procedure will result in such communication being considered as timely if the established date is within the required period for reply. The Certificate should be signed by the individual actually depositing or transmitting the correspondence or by an individual who, upon information and belief, expects the correspondence to be mailed or transmitted in the normal course of business by another no later than the date indicated.

Certificate of Mailing

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to:

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

on _____.
  (Date)

Typed or printed name of person signing this certificate:

_____

Signature: _____

Certificate of Transmission

I hereby certify that this correspondence is being facsimile transmitted to the United States Patent and Trademark Office, Fax No. (703)_____ - _____ on _____.
  (Date)

Typed or printed name of person signing this certificate:

_____

Signature: _____

Please refer to 37 CFR 1.6(d) and 1.8(a)(2) for filing limitations concerning facsimile transmissions and mailing, respectively.
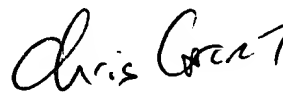
Any inquiry concerning this communication or earlier communications from the examiner should

be directed to Christopher M. Lambrecht whose telephone number is (703) 305-8710. The examiner can

normally be reached on 9:30 AM - 6:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor,

Christopher Grant can be reached on (703) 305-4755. The fax phone number for the organization where

this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application

Information Retrieval (PAIR) system. Status information for published applications may be obtained

from either Private PAIR or Public PAIR. Status information for unpublished applications is available

through Private PAIR only. For more information about the PAIR system, see http://pair-

direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free).

<div style="text-align: right;">

Christopher M. Lambrecht
Examiner
Art Unit 2611

</div>

CML

CHRIS GRANT
PRIMARY EXAMINER